Active Directory Penetration Testing

Course Introduction

Alexis Ahmed

Senior Penetration Tester @HackerSploit
Offensive Security Instructor @INE

Course Topic Overview

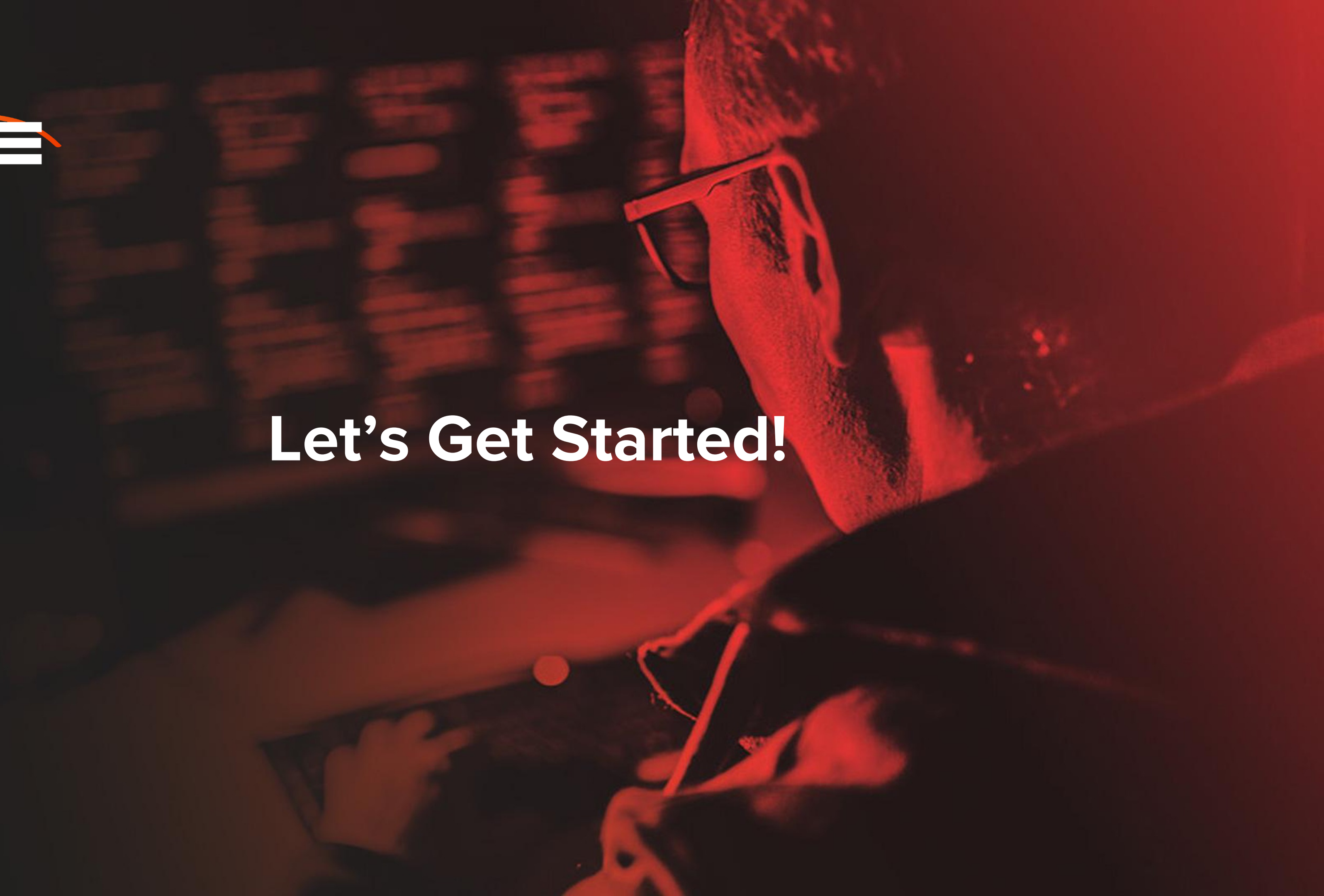
- Active Directory Primer
- Active Directory Penetration Testing
  - Active Directory Pentesting Methodology
- Active Directory Enumeration
  - BloodHound
  - PowerView
- Active Directory Privilege Escalation
  - Kerberos Attacks (Kerberoasting, AS-REP Roasting)
- Active Directory Lateral Movement
  - Pass-the-Hash
  - Pass-the-Ticket
- Active Directory Persistence
  - DCSync
  - Silver Ticket
  - Golden Ticket

Prerequisites

- Basic Understanding of Computer Networking
  - Knowledge of IP addresses, subnetting, routing, and network devices (switches, routers, firewalls).
  - Familiarity with common network protocols (TCP, UDP, HTTP, DNS, etc.).
- Fundamentals of Operating Systems
  - Basic knowledge of Windows and Linux operating systems, including their command-line interfaces.
  - Understanding of system processes, file systems, and user permissions.
- Experience with Exploitation and Post-Exploitation
  - Knowledge and experience in exploitation and post-exploitation on Windows.
  - Ability to target Windows specific ports, protocols and services (SMB, RDP, WinRM etc)
  - Ability to identify and exploit vulnerabilities/misconfigurations in Windows systems.
- Experience with Penetration Testing Tools
  - Some experience using common penetration testing tools (e.g., Metasploit, Nmap, Wireshark).
  - Knowledge and understanding of the penetration testing methodology and lifecycle..

Learning Objectives:

1. Active Directory Fundamentals
   - Understand Active Directory Architecture: Gain a comprehensive understanding of Active Directory components, including domains, domain controllers, forests, trust relationships, OUs and Group Policy Objects (GPOs).
2. Active Directory Penetration Testing Methodology & Process
   - Gain a comprehensive understanding of the Active Directory penetration testing methodology, including the systematic approach to assessing and exploiting vulnerabilities within AD environments.
3. Active Directory Enumeration
   - Conduct reconnaissance and enumeration of Active Directory environments using tools like PowerView and BloodHound to gather information about users, groups, permissions, and trust relationships.
4. Active Directory Privilege Escalation
   - Demonstrate proficiency in leveraging Active Directory privilege escalation techniques like Kerberoasting and AS-REP roasting to escalate privileges and gain unauthorized access to sensitive resources.
5. Active Directory Lateral Movement
   - Demonstrate proficiency in moving laterally within AD environments by leveraging techniques like Pass-the-Hash and Pass-the-Ticket attacks..
6. Active Directory Persistence
   - Demonstrate proficiency in leveraging persistence techniques like Silver Ticket and Golden Ticket attacks in order to maintain access to compromised systems within Active Directory environments.



Let’s Get Started!

Introduction To Active Directory

Introduction To Active Directory

- Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks.

- It serves as a centralized repository for managing and organizing information about network resources, such as users, computers, groups, and other devices.

- Active Directory provides a wide range of services related to identity and access management within a networked environment.

Active Directory Use Cases

- **User Authentication and Authorization:** Active Directory serves as a central authentication and authorization mechanism. Users can log in to their computers or other network resources using their Active Directory credentials, and their access permissions are controlled based on their assigned roles and group memberships.

- **Resource Management:** It enables administrators to efficiently manage and organize network resources such as computers, printers, shared folders, and applications. This centralized management simplifies tasks such as software deployment, configuration management, and access control.

Active Directory Use Cases

- **Group Policy Management:** Active Directory allows administrators to define and enforce security policies, configurations, and settings across all domain-joined devices. Group Policies ensure consistency and security compliance throughout the network.

- **Directory Services:** It provides a hierarchical structure for organizing objects within the network, making it easier to locate and manage resources. This structure includes domains, trees, and forests, allowing organizations to scale their network infrastructure as needed.

Active Directory Components

- **Domains:** A domain is a logical grouping of network objects (such as users, computers, and resources) that share a common directory database and security policies. Domains are administered as a single unit and form the core building blocks of an Active Directory environment.

- **Domain Controllers (DCs):** Domain Controllers are servers that manage access to the resources within a domain. They store a replica of the Active Directory database and authenticate user logins, enforce security policies, and replicate changes to other domain controllers within the domain.

Active Directory Components

- **Forest:** A forest is a collection of one or more domains that share a common schema, configuration, and global catalog. It represents the top-level container in an Active Directory hierarchy and defines the boundaries within which trust relationships are established.

- **Organizational Units (OUs):** OUs are containers within a domain that allow administrators to organize and manage objects more effectively. OUs can be used to delegate administrative tasks, apply Group Policies, and control access permissions at a more granular level than domains.

Active Directory Components

- **Global Catalog (GC):** The Global Catalog is a distributed data repository that contains a partial replica of all objects in the forest. It facilitates cross-domain searches and enables users to locate resources across the entire Active Directory forest.

- **Trust Relationships:** Trust relationships define how authentication and authorization are extended between domains within a forest or between separate forests. Trusts allow users in one domain to access resources in another domain while maintaining security boundaries.

Understanding Active Directory

Example Use Case: Foo Bank Inc

Managing Small Networks

- Let’s start off with a simple example, Imagine yourself deploying and managing a small network consisting of less than 10 Windows computers. In such a small network, setting up, configuring, deploying and managing each computer will be relatively easy.

- You can manually log onto each computer, create user accounts for the employee(s) using the computer, make configuration changes and install/remove software. If a computer stops working or if an employee encounters an issue, you will be able to easily identify and resolve the issue given the small number of computers being managed as well as your intricate knowledge of every system and it’s configuration.

Example Use Case: Foo Bank Inc

Now let's consider a more realistic scenario.

- You have been hired as a system administrator for a medium-sized financial institution, called "Foo Bank Inc", which has around 50 employees, more than 100 computers and operates in from 2 office locations.
- At this point, the previous manual approach will be unfeasible. Could you possibly manage every computer individually within the network, manually set policies for each user across the network, and offer on-site support for everyone? The answer is probably no. This is precisely where Active Directory (AD) becomes essential.
- Here's how Active Directory (AD) can be used for centralization within this organization:

Example Use Case: Foo Bank Inc

- A Windows domain is a collection of computers, servers, users, and devices that are grouped together and managed as a single entity within a network environment.

- In the context of Microsoft's Windows operating system, a domain is established using Active Directory (AD), which serves as the central directory service for authentication, authorization, and resource management.

Authentication & Authorization

- Single Sign-On (SSO): With Active Directory, employees at Foo Bank Inc. can log in to their computers using a single set of credentials (username and password). These credentials are verified centrally by Active Directory, providing a seamless and secure authentication experience.

- Role-Based Access Control (RBAC): AD allows the IT administrators at Foo Bank Inc. to define roles and groups based on job functions or departments. For example, there can be groups like "Accounting", "Marketing", and "Developers". Each group is assigned specific access permissions to network resources, ensuring that employees have access only to the resources relevant to their roles.

Resource Management

- Centralized User and Computer Management: Active Directory provides a central repository for storing information about users, computers, and other network resources. IT administrators can use AD to create, modify, and delete user accounts, manage group memberships, and join computers to the domain, all from a single management console.

- Software Deployment and Updates: Foo Bank Inc. can use Group Policy Objects (GPOs) within Active Directory to deploy software applications, enforce software configurations, and distribute updates to all domain-joined computers automatically. This centralized management simplifies software maintenance and ensures consistency across the organization.

Group Policy Management

- Security Policies: AD allows administrators to define and enforce security policies across the entire organization using Group Policy. For example, they can enforce password complexity requirements, enable BitLocker encryption on company laptops, and restrict access to sensitive files and folders.

- Desktop Configurations: With Group Policy, administrators can standardize desktop configurations, such as desktop backgrounds, screensaver settings, and firewall rules, ensuring a consistent user experience across all computers in the organization.

Directory Services

- Organizational Structure: Foo Bank Inc. can use Organizational Units (OUs) within Active Directory to organize users, computers, and other objects based on departments, teams, or geographical locations. This hierarchical structure makes it easier to manage and delegate administrative tasks within the organization.

- Scalability: As Foo Bank Inc. grows, Active Directory can scale to accommodate the increasing number of users, computers, and resources. New departments or branch offices can be added to the existing Active Directory infrastructure, maintaining centralized management and control.

Users, Groups & Computers

Domain Users

- Security principals refer to entities in the Windows security infrastructure that can be assigned permissions to access various resources within a Windows environment.

- These entities can represent users, groups, computers, or services, and they play a central role in controlling access to resources through security descriptors.

Domain Users

- Users represent individuals who interact with the network. Each user has a unique account within Active Directory, identified by a username and associated with a password. Users use their credentials to log in to computers, access network resources, and perform various tasks.
- User accounts in Active Directory can store information such as full name, email address, phone number, job title, and department. This information can be used for authentication, authorization, and management purposes.
- Administrators can manage user accounts by creating, modifying, or deleting them using Active Directory management tools. They can also assign permissions, group memberships, and other settings to control user access to network resources.

Groups

- Groups are collections of user accounts, computer accounts, or other groups within Active Directory. They provide a convenient way to manage access permissions and apply settings to multiple users or computers simultaneously.
- There are two main types of groups in Active Directory:
  - **Security Groups:** Security groups are used to manage access permissions to network resources. Users can be added to security groups, and permissions can be assigned to these groups to control resource access.
  - **Distribution Groups:** Distribution groups are used for sending email messages to a group of recipients. They do not have security-related permissions and are primarily used for email distribution purposes.

- Group membership allows administrators to apply settings, permissions, and policies to a group of users or computers collectively, rather than individually managing each account.

Security Groups

Security Group	Function
Domain Admins	Domain Admins is one of the most powerful security groups in Active Directory. It is automatically created when the domain is first installed and is granted full administrative control over the entire domain.
Enterprise Admins	Enterprise Admins is a forest-wide security group that holds administrative privileges over all domains within the Active Directory forest.
Server Operators	Server Operators is a security group with permissions to manage domain controllers and member servers within the domain.
Backup Operators	Backup Operators is a security group with permissions to perform backup and restore operations on domain controllers and member servers.
Account Operators	Account Operators is a security group with permissions to manage user accounts, groups, and computer accounts within the domain.

Security Groups

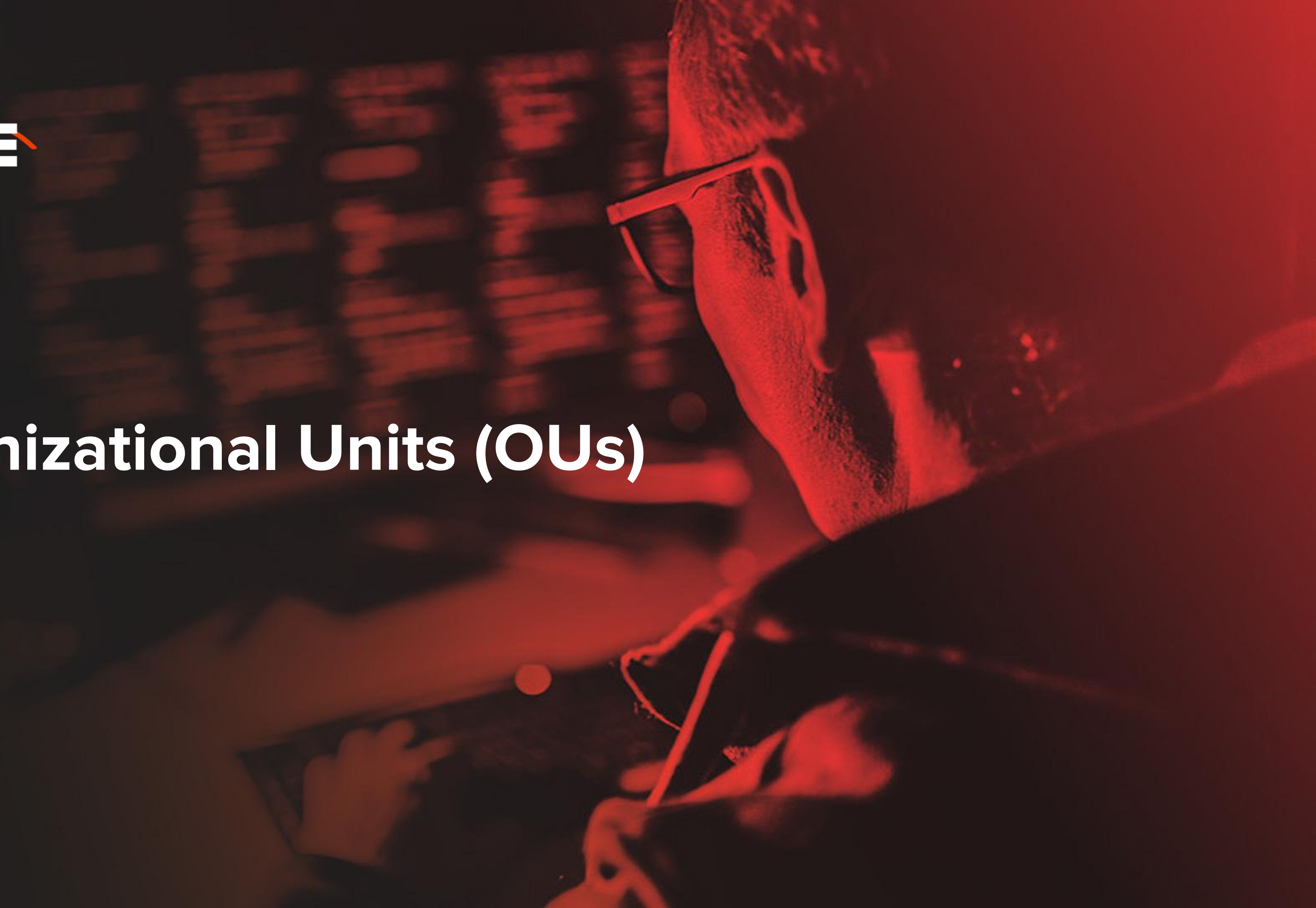
Security Group	Function
Domain Users	Domain users are individual accounts created within the Active Directory domain to represent people who interact with the network. Each user is assigned a unique username and password, which they use to log in to domain-joined computers and access network resources.
Domain Computers	Domain computers are devices, including workstations, laptops, servers, and other networked devices, that are joined to the Active Directory domain. When a computer is joined to the domain, it establishes a trust relationship with the domain and becomes a member of the domain.
Domain Controllers	A Domain Controller (DC) is a server that operates within the Active Directory (AD) environment and is responsible for authenticating users, authorizing access to resources, and maintaining the directory database.

Computers

- Computers represent physical or virtual devices that are joined to the Active Directory domain. This includes workstations, servers, laptops, and other network devices.
- Each computer within the domain has a corresponding computer account in Active Directory, identified by a unique name. When a computer joins the domain, a secure trust relationship is established between the computer and the domain, allowing the computer to authenticate users and access network resources.
- Computer accounts in Active Directory store information such as the computer name, domain membership status, operating system version, and last login time. Administrators can manage computer accounts by adding, removing, or modifying them using Active Directory management tools.

Demo: Users, Groups & Computers

Organizational Units (OUs)



Organizational Units (OUs)

- OUs are containers within an Active Directory domain used to organize and manage objects such as user accounts, computer accounts, groups, and other OUs.
- They provide a hierarchical structure for organizing and delegating administrative control over objects in the directory.
- OUs are used to organize objects in a logical manner based on administrative, geographical, or departmental criteria.
- They simplify administration by allowing administrators to apply Group Policy settings, permissions, and other configurations to multiple objects at once.

Organizational Units (OUs)

- OUs can contain users, groups, computers, and other OUs, creating a hierarchical structure that reflects the organization's structure.

- They can have Group Policy Objects (GPOs) linked to them to apply specific configurations to objects within the OU.

- Administrative tasks, such as delegating control and setting permissions, can be assigned to specific OUs to distribute administrative responsibilities.

Difference Between OUs & Security Groups

- OUs are used for organizing and managing objects within Active Directory, while Security Groups are used for access control and permissions management.
- OUs create a hierarchical structure for organizing objects, while Security Groups can be organized in a flat structure.
- OUs are containers for objects within Active Directory and can contain other OUs, while Security Groups are collections of users, computers, or other groups.
- OUs are used for administrative delegation, Group Policy application, and object organization, while Security Groups are used for access control and defining permissions.

Demo: Organizational Units (OUs)

Active Directory Authentication

Active Directory Authentication

- Active Directory (AD) authentication is the process by which users and computers verify their identities to gain access to network resources within an Active Directory domain.

- It plays a critical role in ensuring secure access to resources while maintaining centralized control over authentication and access management.

- As far as authentication on Active Directory is concerned, the most common way for users to authenticate is by providing a username and password.

Active Directory Authentication

- Active Directory (AD) supports several authentication protocols that facilitate secure communication and user authentication within an AD domain environment.

- These protocols play a crucial role in ensuring the confidentiality, integrity, and authenticity of authentication exchanges. Here are some of the key AD authentication protocols:
  - Kerberos
  - NTLM

Kerberos

Kerberos is the primary authentication protocol used by Active Directory for user authentication.

How it works:

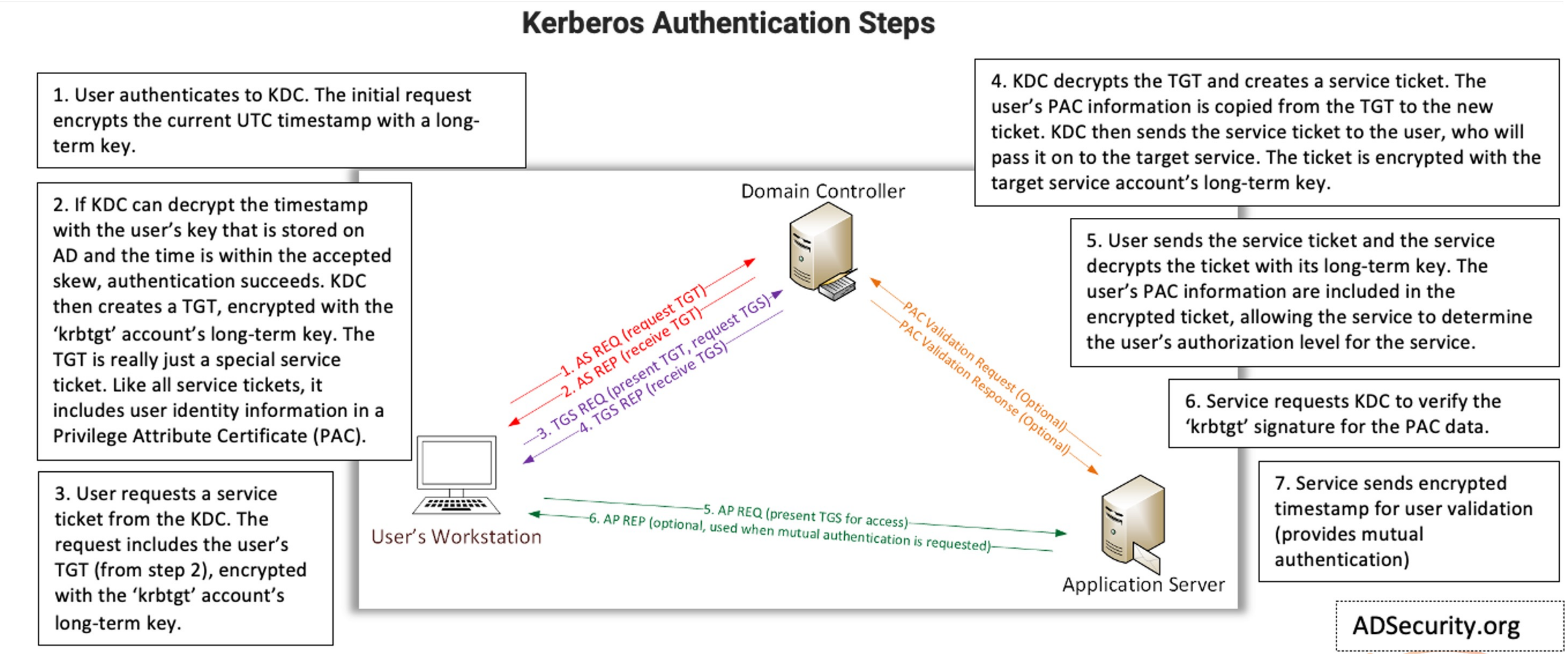
- When a user attempts to log in, their client computer requests a Ticket Granting Ticket (TGT) from the Key Distribution Center (KDC), which is typically a domain controller.
- The domain controller verifies the user's credentials and issues a TGT if authentication is successful.
- The TGT is then used to obtain Service Tickets for accessing specific network resources.

Kerberos

Features:

- Mutual authentication: Both the client and the server verify each other's identities.
- Single Sign-On (SSO): Users authenticate once and can access multiple resources without re-entering credentials.
- Ticket-based: Authentication exchanges rely on encrypted tickets, reducing the risk of credential theft.

Kerberos Authentication



Kerberos Authentication Steps

1. User authenticates to KDC. The initial request encrypts the current UTC timestamp with a long-term key.

2. If KDC can decrypt the timestamp with the user's key that is stored on AD and the time is within the accepted skew, authentication succeeds. KDC then creates a TGT, encrypted with the 'krbtgt' account's long-term key. The TGT is really just a special service ticket. Like all service tickets, it includes user identity information in a Privilege Attribute Certificate (PAC).

3. User requests a service ticket from the KDC. The request includes the user's TGT (from step 2), encrypted with the 'krbtgt' account's long-term key.

4. KDC decrypts the TGT and creates a service ticket. The user's PAC information is copied from the TGT to the new ticket. KDC then sends the service ticket to the user, who will pass it on to the target service. The ticket is encrypted with the target service account's long-term key.

5. User sends the service ticket and the service decrypts the ticket with its long-term key. The user's PAC information are included in the encrypted ticket, allowing the service to determine the user's authorization level for the service.

6. Service requests KDC to verify the 'krbtgt' signature for the PAC data.

7. Service sends encrypted timestamp for user validation (provides mutual authentication)

Domain Controller
1. AS REQ (request TGT)
2. AS REP (receive TGT)
3. TGS REQ (present TGT, request TGS)
4. TGS REP (receive TGS)
PAC Validation Request (Optional)
PAC Validation Response (Optional)
User's Workstation
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)
Application Server

ADSecurity.org

NTLM

NTLM is an older authentication protocol used by Windows systems for backward compatibility.

How it works:

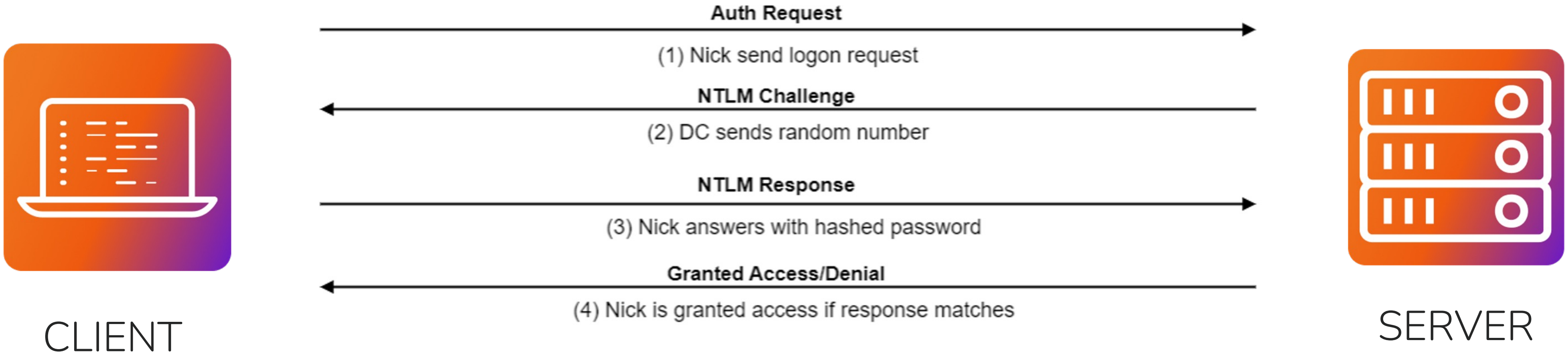
- When a user attempts to log in, their client computer sends a hashed version of their password to the server.
- The server compares the hash to the stored hash of the user's password.
- If the hashes match, authentication is successful.

NTLM

Features:

- Compatibility: NTLM is supported by older Windows systems and applications.
- Simplicity: NTLM authentication does not require the complexity of Kerberos, making it easier to implement in certain environments.
- Security: NTLM has security limitations compared to Kerberos, including susceptibility to pass-the-hash attacks and lack of mutual authentication.

NTLM



CLIENT

Auth Request

(1) Nick send logon request

NTLM Challenge

(2) DC sends random number

NTLM Response

(3) Nick answers with hashed password

Granted Access/Denial

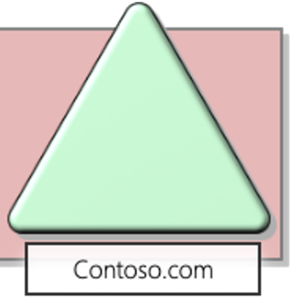
(4) Nick is granted access if response matches

SERVER

Trees, Forests & Trusts

Domains

Domains are used to group and manage objects in an organization

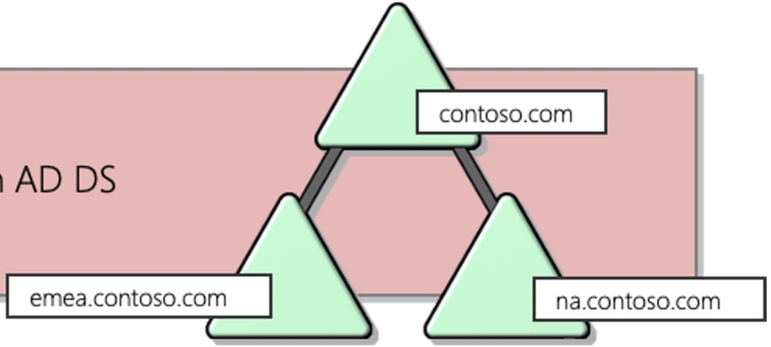


Domains:

- An administrative boundary for applying policies to groups of objects
- A replication boundary for replicating data between domain controllers
- An authentication and authorization boundary that provides a way to limit the scope of access to resources

Trees

A domain tree is a hierarchy of domains in AD DS

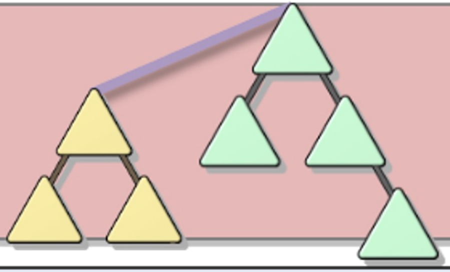


All domains in the tree:

- Share a contiguous namespace with the parent domain
- Can have additional child domains
- By default create a two-way transitive trust with other domains

Forests

A forest is a collection of
one or more domain trees

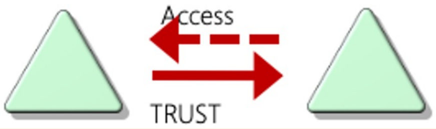
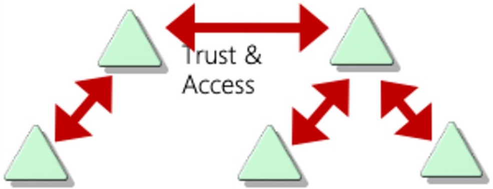


Forests:

- Share a common schema
- Share a common configuration partition
- Share a common global catalog to enable searching
- Enable trusts between all domains in the forest
- Share the Enterprise Admins and Schema Admins groups

Trusts

Trusts provide a mechanism for users to gain access to resources in another domain

Types of Trusts	Description	Diagram
Directional	The trust direction flows from trusting domain to the trusted domain	
Transitive	The trust relationship is extended beyond a two-domain trust to include other trusted domains	

- All domains in a forest trust all other domains in the forest
- Trusts can extend outside the forest

Trusts

Things to note regarding AD Trusts:

- Domains can allow access to shared resources outside of their boundaries by using a trust. Forest trusts allow users to access resources in any domain in the other forest, as well as logon to any domain in the forest.

AD Penetration Testing Methodology

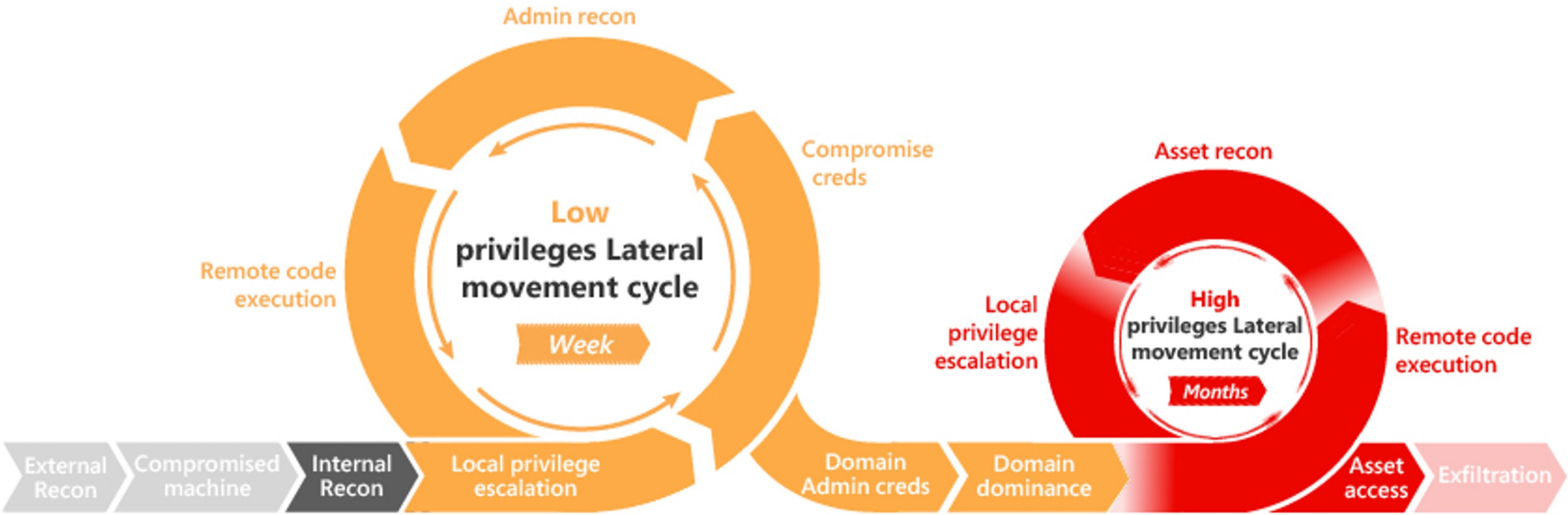
Active Directory Penetration Testing

- Active Directory (AD) penetration testing is a security assessment process aimed at evaluating the security posture of an organization's Active Directory infrastructure.

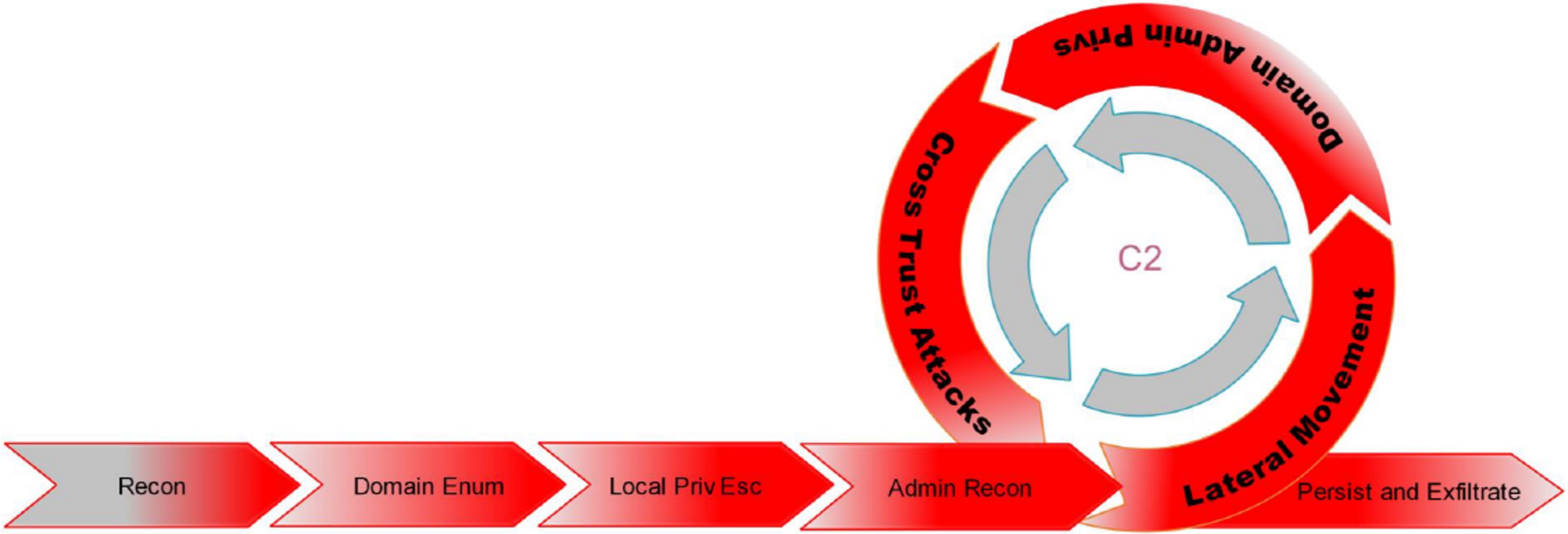
- Active Directory, developed by Microsoft, is a directory service that provides centralized authentication, authorization, and management of network resources in Windows environments.

- Penetration testing of Active Directory involves simulating real-world attacks to identify vulnerabilities, weaknesses, and misconfigurations that could compromise the security of the AD environment.

Active Directory Kill Chain



Active Directory Kill Chain #2



AD Pentesting Methodology

- Initial Compromise
- Host Reconnaissance
- Domain Enumeration
- Local Privilege Escalation
- Administrator Enumeration
- Lateral Movement
- Domain Admin privs
- Cross Trust Attacks
- Domain Persistence
- Exfiltrate

AD Penetration Testing Methodology

Breaching AD

Techniques

- Password Spraying: Attempt to authenticate using common or leaked passwords across multiple user accounts.
- Brute Force Attacks: Use automated tools to guess passwords for user accounts with weak or default passwords.
- Phishing: Craft convincing emails to trick users into revealing their credentials or executing malicious attachments.
- Poisoning: LLMNR/NBT-NS Poisoning

AD Penetration Testing Methodology

AD Enumeration

Techniques

- PowerView: Enumerate AD objects, attributes, and permissions to identify potential security weaknesses.
- BloodHound: Visualize and analyze AD permissions, group memberships, and attack paths.
- LDAP Enumeration: Query the AD LDAP service to retrieve detailed information about users, groups, computers, and OUs.

AD Penetration Testing Methodology

Privilege Escalation

Techniques

- Kerberoasting: Kerberoasting is a Kerberos attack that targets service accounts to obtain their encrypted service account passwords (SPNs), which can be cracked offline to obtain plaintext passwords.
- AS-REP Roasting: AS-REP roasting is a Kerberos authentication attack that targets user accounts with the "Do not require Kerberos preauthentication" attribute set.

AD Penetration Testing Methodology

Lateral Movement

Techniques:

- Pass-the-Hash: Use stolen password hashes to authenticate and gain access to other systems without knowing the plaintext passwords.
- Pass-the-ticket (PtT) is a technique used in Active Directory environments to authenticate to other systems or services using stolen Kerberos ticket-granting tickets (TGTs) or service tickets without knowing the user's plaintext password.

AD Penetration Testing Methodology

Persistence

Techniques:

- Silver Ticket: A Silver Ticket attack is a technique used in Active Directory (AD) environments to impersonate any service or computer account by forging Kerberos service tickets without the need to obtain the account's plaintext password.
- Golden Ticket: Golden ticket attacks involve forging Kerberos tickets for arbitrary users, allowing attackers to impersonate any user and access any resource within the AD environment.

References & Resources

- Ocd-mindmaps: https://orange-cyberdefense.github.io/ocd-mindmaps/
- Active Directory Exploitation Cheatsheet: https://github.com/S1ckB0y1337/Active-Directory-Exploitation-Cheat-Sheet

Password Spraying

Password Spraying

- Password spraying is an attack technique in which an adversary attempts to compromise user accounts by trying to authenticate with a curated list of passwords that are either frequently used or likely to be used by their target.

- Password spraying can be conducted by an external adversary against any internet-facing system or SaaS application, or by an adversary that has gained a foothold within the network and is seeking to widen their access.

- Frequent targets for password spraying include VPN servers, web-based email applications and single sign-on providers.

Password Spraying

- Unlike credential stuffing where an adversary is targeting specific users with previously compromised passwords, password spraying is about trying common or likely passwords against as many users as possible.

- Thus, many adversaries structure their attacks to avoid detection, perhaps trying only one password for each user account at a time or waiting some time between attempts.

Lab Environment

- In this lab environment, GUI access to a Domain User called Research/Student on a Windows Server 2012 machine, which serves as your workstation. This workstation contains vulnerabilities that are susceptible to password spraying attacks - a common method for guessing passwords that often yield results due to the habitual use of simple and predictable passwords within the Active Directory setup.

- Your task is to perform a password spraying attack aiming to identify weak passwords, which could potentially provide you with escalated privileges, even up to the level of domain admin access.

Lab Environment

Objective: Execute a password spraying attack to discover weak passwords within the Active Directory.

Below are the tasks that you need to perform:

- Task 1: Identify all the users in the domain.
- Task 2: Initiate the Password Spraying Attack.
- Task 3: Execution and Verification of the Password Spraying Attack.

Lab Demo: Password Spraying

AD Enumeration: BloodHound

AD Enumeration With BloodHound

- Active Directory (AD) reconnaissance is a crucial step in assessing the security of an Active Directory environment.

- It involves gathering information about the Active Directory infrastructure to identify potential vulnerabilities and security weaknesses. One powerful tool for conducting such reconnaissance is BloodHound.

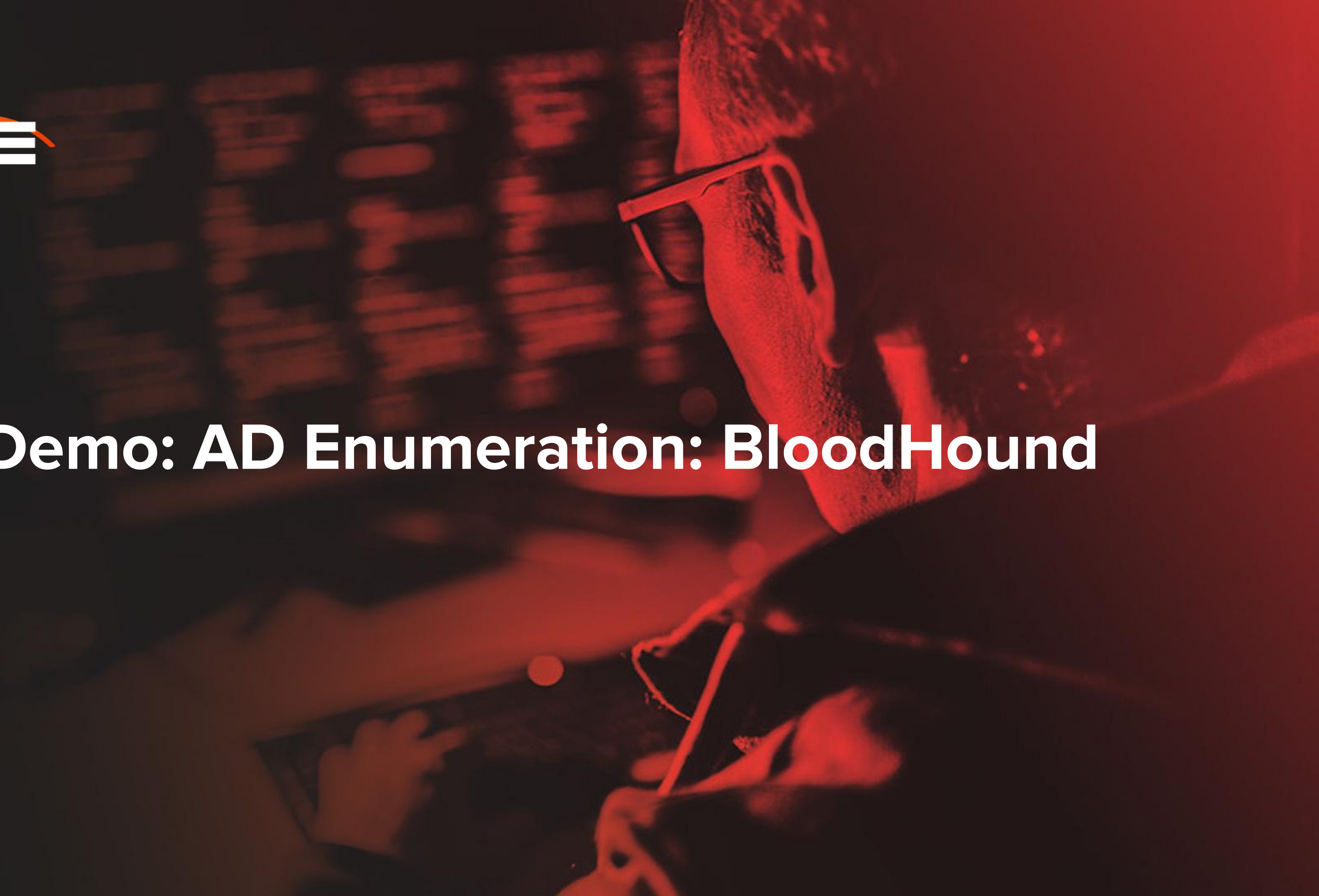
AD Enumeration With BloodHound

- BloodHound is a single page Javascript web application, built on top of Linkurious, compiled with Electron, with a Neo4j database fed by a C# or PowerShell data collector.
- BloodHound uses graph theory to reveal the hidden and often unintended relationships within an Active Directory or Azure environment.
- Attackers can use BloodHound to easily identify highly complex attack paths that would otherwise be impossible to quickly identify. Defenders can use BloodHound to identify and eliminate those same attack paths. Both blue and red teams can use BloodHound to easily gain a deeper understanding of privilege relationships in an Active Directory or Azure environment.

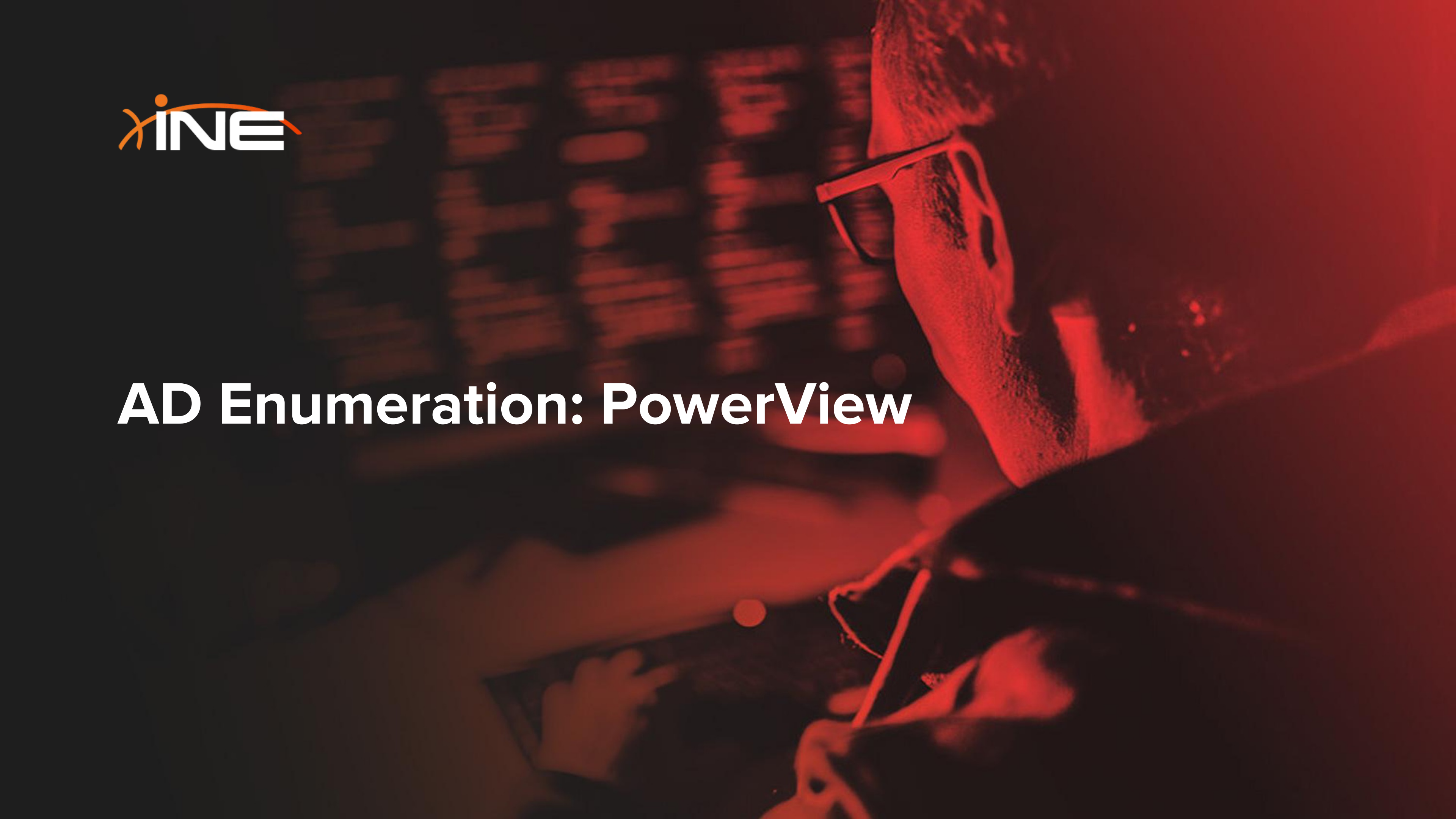
Lab Environment

- In this lab environment, you will be provided with GUI access to a Windows machine (2012). This machine will serve as your attacker machine.

- Your task in this lab is to enumerate the Active Directory environment using BloodHound.



Lab Demo: AD Enumeration: BloodHound



AD Enumeration: PowerView

Lab Demo: AD Enumeration: PowerView

AS-REP Roasting

AS-REP Roasting

- AS-REP Roasting is a technique used to exploit a weakness in the Kerberos authentication protocol.

- Kerberos is commonly used in Windows Active Directory environments for authentication purposes. AS-REP Roasting specifically targets a vulnerability in the way Kerberos handles authentication requests.

- In the Kerberos protocol, when a user wants to authenticate to a service, they send an Authentication Service Request (AS-REQ) to the Key Distribution Center (KDC). The KDC then responds with an Authentication Service Reply (AS-REP), which includes a ticket-granting ticket (TGT). The TGT is encrypted using the user's password hash.

AS-REP Roasting

- AS-REP Roasting takes advantage of the fact that some user accounts in Active Directory may have the "Do not require Kerberos preauthentication" option enabled.

- This option allows the AS-REP to be requested without the need for the user's password.

- An attacker can identify these vulnerable accounts by querying the Active Directory for accounts with this option enabled.

Lab Environment

- In this lab environment, GUI access to a Domain user called Research/Student on a Windows Server 2012 machine, which serves as your workstation. The workstation is vulnerable to AS-REP Roasting attack.

- Your task is to identify accounts with the "Do not require Kerberos preauthentication" option enabled in Active Directory.

- By exploiting this vulnerability, you aim to capture AS-REP responses, extract password hashes, and crack the hash of another domain user in the Active Directory domain.

Lab Environment

Objective: Identify accounts vulnerable to AS-REP Roasting and gain access to another domain user within Active Directory.

Below are the tasks that you need to perform:

- Task 1: Identify vulnerable account with enabled "Do not require preauthentication" option.
- Task 2: Exploit AS-REP Roasting to extract password hashes.
- Task 3: Crack hashes for plaintext passwords.

Lab Demo: AS-REP Roasting

Kerberoasting

Kerberoasting

- Kerberoasting is a post-exploitation attack technique that attempts to obtain a password hash of an Active Directory account that has a Service Principal Name ("SPN").

- In such an attack, an authenticated domain user requests a Kerberos ticket for an SPN. The retrieved Kerberos ticket is encrypted with the hash of the service account password affiliated with the SPN. (An SPN is an attribute that ties a service to a user account within the AD). The adversary then works offline to crack the password hash, often using brute force techniques.

- Once the plaintext credentials of the service account are obtained, the adversary can impersonate the account owner and inherit access to any systems, assets or networks granted to the compromised account.

Lab Environment

- In this lab environment, GUI access to a Domain User called Research/Student on a Windows Server 2012 machine, which serves as your workstation. The workstation is vulnerable to Kerberoasting attack.

- Your task is to identify accounts that have a Service Principal Name (“SPN”) enabled, allowing the attacker to request TGS tickets and extract the password hashes.

- By exploiting this, you will aim to gain the cracked password for the identified account helping us to compromise data or escalate privileges in the Active Directory environment.

Lab Environment

Objective: Identify user accounts with Service Principal Name (SPN) enabled, perform a Kerberoasting attack to extract password hashes, and use the cracked password to compromise data or escalate privileges within the Active Directory.

Below are the tasks that you need to perform:

- Task 1: Identify user accounts with Service Principal Name (SPN) enabled.
- Task 2: Request a TGS ticket for the specified SPN using Kerberos.
- Task 3: Crack the password from the TGS ticket using Tgsrepcrack.

Lab Demo: Kerberoasting

AD Lateral Movement: Pass-the-Hash

AD Lateral Movement: Pass-the-Hash

- A Pass-the-Hash (PtH) attack is a credential theft technique primarily targeting Windows-based systems. In this attack, an attacker obtains the hashed password of a user and uses it to authenticate as that user, bypassing the need for the actual plain-text password.

- The attack typically starts with the attacker gaining unauthorized access to a compromised system where the target user's hashed password is stored. Once the hash is acquired, the attacker can exploit weaknesses in the Windows authentication protocol, such as NTLM or Kerberos, to pass the hashed credentials to other systems within the Active Directory domain.

- By bypassing the need to crack the password, the attacker can move laterally within the network, escalate privileges, and potentially carry out malicious activities.

Lab Environment

- In this lab environment, you will be provided with GUI access to a Windows machine (2012). This machine will serve as your attacker machine. Your task in this lab is to perform Pass-the-Hash attack to gain access to the Domain Controller.

- Objective: Perform Pass-the-Hash attack to gain access to the Domain Controller.

- Note: All the tools are present in the C:\Tools directory.

Lab Demo: AD Lateral Movement: Pass-the-Hash

AD Lateral Movement: Pass-the-Ticket

AD Lateral Movement: Pass-the-Ticket

- Pass the Ticket is a credential theft technique that enables adversaries to use stolen Kerberos tickets to authenticate to resources (e.g., file shares and other computers) as a user without having to compromise that user's password. Adversaries often use this technique to move laterally through an organization's network to hunt for opportunities to escalate their privileges or fulfil their mission.

- Both ticket-granting service (TGS) tickets and ticket-granting tickets (TGT) can be stolen and reused by adversaries. Without administrative privileges, an adversary can obtain the TGT (using "fake delegation") and all TGS tickets for the current user.

- With administrative privileges, an adversary can dump the LSASS process and obtain all TGTs and TGS tickets cached on the system.

Lab Environment

- In this lab environment, GUI access to a Domain User called Research/Student on a Windows Server 2012 machine, which serves as your workstation. The workstation is vulnerable to Pass the Ticket attack.

- Your task is to execute a Pass-The-Ticket attack. By performing this attack, you will impersonate a user's session by reusing the Kerberos tickets, with the ultimate aim of accessing resources and escalating privileges within the Active Directory environment.

Lab Environment

Objective: Execute a Pass-The-Ticket (PtT) attack by impersonating a user session, and gaining unauthorized access to escalate privileges within the Active Directory environment.

Below are the tasks that you need to perform:

- Task 1: Conducting Reconnaissance
- Task 2: Attack Implementation
- Task 3: Export Kerberos ticket
- Task 4: Check Domain Controller Access

Lab Demo: AD Lateral Movement: Pass-the-Ticket

AD Persistence: Silver Ticket

AD Persistence: Silver Ticket

- The Silver ticket attack involves the creation of a valid Ticket Granting Service (TGS) for a specific service when the password hash of the service is obtained. This allows unauthorized access to the service by forging a customized TGS.

- Silver tickets have a narrower scope compared to Golden tickets, as they only provide access to a specific resource (e.g., MSSQL) and the system hosting that resource. However, adversaries capable of forging Silver tickets can create and use TGS tickets without interacting with the Key Distribution Center (KDC), potentially making detection more challenging.

AD Persistence: Silver Ticket

- If the target service operates under a user account context, like MSSQL, the password hash of the service account is required for Silver Ticket creation.

- In addition to user accounts, computers themselves host services, with the most common example being the Windows file share that utilizes the "CIFS" service.

- In the case of a computer-hosted service, the associated computer account's password hash is the essential data needed to generate a Silver Ticket.

Lab Environment

- In this lab environment, you will be provided with GUI access to a Windows machine (2012). This machine will serve as your attacker machine. Your task in this lab is to generate a Silver ticket, targeting the CIFS service on the Domain Controller.

- Objective: Perform a Silver ticket attack targeting the CIFS service on the Domain Controller.

Lab Demo: AD Persistence: Silver Ticket

AD Persistence: Golden Ticket

AD Persistence: Golden Ticket

- A Golden Ticket attack is a malicious cybersecurity attack in which a threat actor attempts to gain almost unlimited access to an organization’s domain (devices, files, domain controllers, etc.) by accessing user data stored in Microsoft Active Directory (AD). It exploits weaknesses in the Kerberos identity authentication protocol, which is used to access the AD, allowing an attacker to bypass normal authentication.

- As an increasing number of companies shift both to the cloud and a remote-first setting, the attack surface has grown beyond the traditional perimeter, with employees logging into company systems using their own devices and networks. This in turn has increased the risk that attackers will be able to break into a network and use a Golden Ticket attack to gain access.

Lab Environment

- In this lab environment, GUI access to Windows Server 2012 machine acts as your workstation. You are logged in with the Domain User account "Research/Student". This workstation has been configured with vulnerabilities linked to Golden Ticket attacks - a potent form of Kerberos manipulation, providing a real-world scenario to practice your cybersecurity skills.

- Your task is to simulate a 'Golden Ticket' attack to exploit the Kerberos ticket-granting ticket (TGT). If executed successfully, you could gain extensive privileges and control over the Active Directory domain.

Lab Environment

Objective: Simulate a Kerberos: Golden Ticket attack to generate a ticket-granting ticket, and escalate privileges to obtain domain controller access.

Below are the tasks that you need to perform:

- Task 1: Extract Administrator's NTML Hash
- Task 2: Execute Pass-the-Hash Attack
- Task 3: Retrieve KRBTGT Account Hash
- Task 4: Generate and Implement a Golden Ticket
- Task 5: Validate Access to Domain Controller

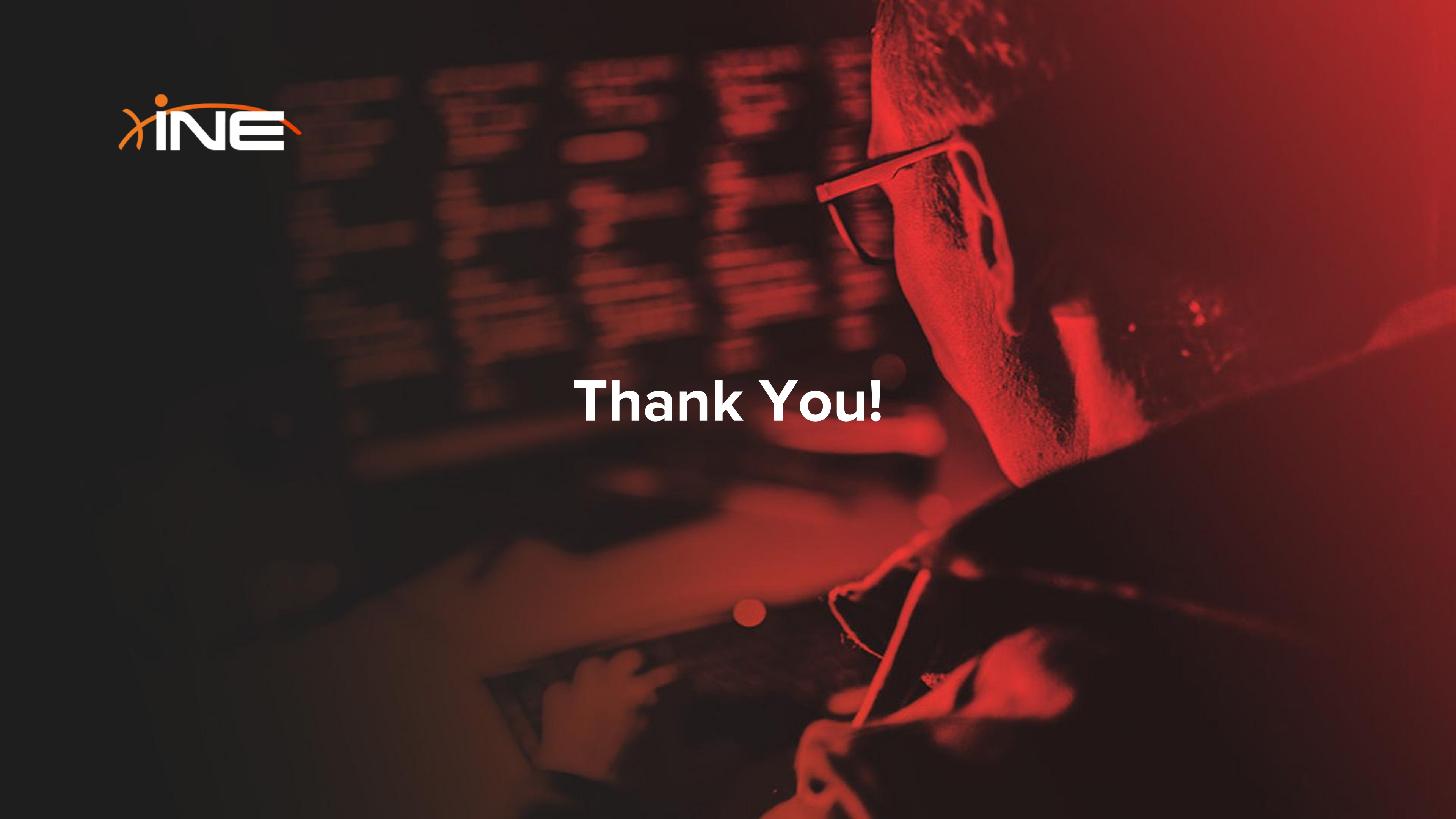
Lab Demo: AD Persistence: Golden Ticket

Active Directory Penetration Testing

Course Conclusion

Learning Objectives:

1. Active Directory Fundamentals
   - Understand Active Directory Architecture: Gain a comprehensive understanding of Active Directory components, including domains, domain controllers, forests, trust relationships, OUs and Group Policy Objects (GPOs).
2. Active Directory Penetration Testing Methodology & Process
   - Gain a comprehensive understanding of the Active Directory penetration testing methodology, including the systematic approach to assessing and exploiting vulnerabilities within AD environments.
3. Active Directory Enumeration
   - Conduct reconnaissance and enumeration of Active Directory environments using tools like PowerView and BloodHound to gather information about users, groups, permissions, and trust relationships.
4. Active Directory Privilege Escalation
   - Demonstrate proficiency in leveraging Active Directory privilege escalation techniques like Kerberoasting and AS-REP roasting to escalate privileges and gain unauthorized access to sensitive resources.
5. Active Directory Lateral Movement
   - Demonstrate proficiency in moving laterally within AD environments by leveraging techniques like Pass-the-Hash and Pass-the-Ticket attacks..
6. Active Directory Persistence
   - Demonstrate proficiency in leveraging persistence techniques like Silver Ticket and Golden Ticket attacks in order to maintain access to compromised systems within Active Directory environments.



Thank You!

EXPERTS AT MAKING YOU AN EXPERT

INE